Course 311: Michaelmas Term 2005
Part II: Topics in Group Theory

D. R. Wilkins

Contents

2 Topics in Group Theory

2.1 Groups

A *binary operation* $*$ on a set G associates to elements x and y of G a third element $x * y$ of G. For example, addition and multiplication are binary operations of the set of all integers.

Definition A *group* G consists of a set G together with a binary operation $*$ for which the following properties are satisfied:

- $(x * y) * z = x * (y * z)$ for all elements x, y, and z of G (the *Associative Law*);
- there exists an element e of G (known as the *identity element* of G) such that $e * x = x = x * e$, for all elements x of G;
- for each element x of G there exists an element x' of G (known as the *inverse* of x) such that $x * x' = e = x' * x$ (where e is the identity element of G).

The *order* $|G|$ of a finite group G is the number of elements of G.

A group G is *Abelian* (or *commutative*) if $x * y = y * x$ for all elements x and y of G.

One usually adopts *multiplicative notation* for groups, where the product $x * y$ of two elements x and y of a group G is denoted by xy. The associative property then requires that $(xy)z = x(yz)$ for all elements x, y and z of G. The identity element is often denoted by e (or by e_G when it is necessary to specify explicitly the group to which it belongs), and the inverse of an element x of G is then denoted by x^{-1}.

It is sometimes convenient or customary to use additive notation for certain groups. Here the group operation is denoted by $+$, the identity element of the group is denoted by 0, the inverse of an element x of the group is denoted by $-x$. By convention, additive notation is rarely used for non-Abelian groups. When expressed in additive notation the axioms for a Abelian group require that $(x + y) + z = x + (y + z)$, $x + y = y + x$, $x + 0 = 0 + x = x$ and $x + (-x) = (-x) + x = 0$ for all elements x, y and z of the group.

We shall usually employ multiplicative notation when discussing general properties of groups. Additive notation will be employed for certain groups (such as the set of integers with the operation of addition) where this notation is the natural one to use.

2.2 Examples of Groups

The sets of integers, rational numbers, real numbers and complex numbers are Abelian groups, where the group operation is the operation of addition.

The sets of non-zero rational numbers, non-zero real numbers and non-zero complex numbers are also Abelian groups, where the group operation is the operation of multiplication.

For each positive integer m the set $\mathbb{Z}_m$ of congruence classes of integers modulo m is a group, where the group operation is addition of congruence classes.

For each positive integer m the set $\mathbb{Z}_m^*$ of congruence classes modulo m of integers coprime to m is a group, where the group operation is multiplication of congruence classes.

In particular, for each prime number p the set $\mathbb{Z}_p^*$ of congruence classes modulo p of integers not divisible by p is a group, where the group operation is multiplication of congruence classes.

For each positive integer n the set of all nonsingular $n \times n$ matrices is a group, where the group operation is matrix multiplication. These groups are not Abelian when $n \geq 2$.

Let E^n denote n-dimensional Euclidean space, so that E^2 denotes the Euclidean plane, and E^3 denotes three-dimensional Euclidean space. A geometrical figure may be represented as a subset S of E^n. A *symmetry* of S is a transformation $T\colon E^n \to E^n$ of E^n which sends straight lines to straight lines, preserves all lengths and angles, and has the property that $T(S) = S$. The collection of all symmetries of a geometrical figure is a group, the *symmetry group of* S, the group operation being that of composition of transformations.

For any natural number n greater than 2, the the *dihedral group* D_{2n} of order $2n$ is defined to be the symmetry group of a regular n-sided polygon in the Euclidean plane. It consists of rotations though an angle of $2\pi j/n$ about the centre of the polygon for $j = 0, 1, 2, \ldots, n-1$, together with the reflections in the n axes of symmetry of the polygon.

The symmetries of a rectangle that is not a square constitute a group of order 4. This group consists of the identity transformation, reflection in the axis of symmetry joining the midpoints of the two shorter sides, reflection in the axis of symmetry joining the two longer sides, and rotation though an angle of π radians (180°). If I denotes the identity transformation, A and B denote the reflections in the two axes of symmetry, and C denotes the rotation through π radians then $A^2 = B^2 = C^2 = I$, $AB = BA = C$, $AC = CA = B$ and $BC = CB = A$. This group is Abelian: it is often referred to as the *Klein 4-group* (or, in German, *Kleinsche Viergruppe*).

The symmetries of a regular tetrahedron in 3-dimensional space constitute

a group. Any permutation of the vertices of the tetrahedron can be effected by an appropriate symmetry of the tetrahedron. Moreover each symmetry is completely determined by the permutation of the vertices which it induces. Therefore the group of symmetries of a regular tetrahedron is of order 24, since there are 24 permutations of a set with four elements. It turns out that this group is non-Abelian.

2.3 Elementary Properties of Groups

In what follows, we describe basic properties of a group G, using multiplicative notation and denoting the identity element of the group by the letter e.

Lemma 2.1 *A group G has exactly one identity element e satisfying $ex = x = xe$ for all $x \in G$.*

Proof Suppose that f is an element of G with the property that $fx = x$ for all elements x of G. Then in particular $f = fe = e$. Similarly one can show that e is the only element of G satisfying $xe = x$ for all elements x of G. ∎

Lemma 2.2 *An element x of a group G has exactly one inverse x^{-1}.*

Proof We know from the axioms that the group G contains at least one element x^{-1} which satisfies $xx^{-1} = e$ and $x^{-1}x = e$. If z is any element of G which satisfies $xz = e$ then $z = ez = (x^{-1}x)z = x^{-1}(xz) = x^{-1}e = x^{-1}$. Similarly if w is any element of G which satisfies $wx = e$ then $w = x^{-1}$. In particular we conclude that the inverse x^{-1} of x is uniquely determined, as required. ∎

Lemma 2.3 *Let x and y be elements of a group G. Then $(xy)^{-1} = y^{-1}x^{-1}$.*

Proof It follows from the group axioms that

$$(xy)(y^{-1}x^{-1}) = x(y(y^{-1}x^{-1})) = x((yy^{-1})x^{-1}) = x(ex^{-1}) = xx^{-1} = e.$$

Similarly $(y^{-1}x^{-1})(xy) = e$, and thus $y^{-1}x^{-1}$ is the inverse of xy, as required. ∎

Note in particular that $(x^{-1})^{-1} = x$ for all elements x of a group G, since x has the properties that characterize the inverse of the inverse x^{-1} of x.

Given an element x of a group G, we define x^n for each positive integer n by the requirement that $x^1 = x$ and $x^n = x^{n-1}x$ for all $n > 1$. We also define $x^0 = e$, where e is the identity element of the group, and we define x^{-n} to be the inverse of x^n for all positive integers n.

Theorem 2.4 *Let x be an element of a group G. Then $x^{m+n} = x^m x^n$ and $x^{mn} = (x^m)^n$ for all integers m and n.*

Proof The identity $x^{m+n} = x^m x^n$ clearly holds when $m = 0$ and when $n = 0$. The identity $x^{m+n} = x^m x^n$ can be proved for all positive integers m and n by induction on n. The identity when m and n are both negative then follows from the identity $x^{-m-n} = x^{-n}x^{-m}$ on taking inverses. The result when m and n have opposite signs can easily be deduced from that where m and n both have the same sign.

The identity $x^{mn} = (x^m)^n$ follows immediately from the definitions when $n = 0$, 1 or -1. The result when n is positive can be proved by induction on n. The result when n is negative can then be obtained on taking inverses. ∎

If additive notation is employed for an Abelian group then the notation 'x^n' is replaced by 'nx' for all integers n and elements x of the group. The analogue of Theorem 2.4 then states that $(m+n)x = mx + nx$ and $(mn)x = m(n(x))$ for all integers m and n.

The associative law may be generalized to products of four or more elements of a group.

Example Given four elements x_1, x_2, x_3 and x_4 of a group, the products

$$((x_1x_2)x_3)x_4, \quad (x_1x_2)(x_3x_4), \quad (x_1(x_2x_3))x_4, \quad x_1((x_2x_3)x_4), \quad x_1(x_2(x_3x_4))$$

all have the same value. (Note that $x_1x_2x_3x_4$ is by definition the value of the first of these expressions.)

Two expressions, each specifying a finite product of elements of a group G, determine the same element of G if the same elements of G occur in both expressions, and in the same order. This result can be proved by induction on the number of elements of G making up such a product.

2.4 Subgroups

Definition Let G be a group, and let H be a subset of G. We say that H is a *subgroup* of G if the following conditions are satisfied:

- the identity element of G is an element of H;
- the product of any two elements of H is itself an element of H;
- the inverse of any element of H is itself an element of H.

A subgroup H of G is said to be *proper* if $H \neq G$.

Lemma 2.5 *Let x be an element of a group G. Then the set of all elements of G that are of the form x^n for some integer n is a subgroup of G.*

Proof Let $H = \{x^n : n \in \mathbb{Z}\}$. Then the identity element belongs to H, since it is equal to x^0. The product of two elements of H is itself an element of H, since $x^m x^n = x^{m+n}$ for all integers m and n (see Theorem 2.4). Also the inverse of an element of H is itself an element of H since $(x^n)^{-1} = x^{-n}$ for all integers n. Thus H is a subgroup of G, as required. ∎

Definition Let x be an element of a group G. The *order* of x is the smallest positive integer n for which $x^n = e$. The subgroup *generated* by x is the subgroup consisting of all elements of G that are of the form x^n for some integer n.

Lemma 2.6 *Let H and K be subgroups of a group G. Then $H \cap K$ is also a subgroup of G.*

Proof The identity element of G belongs to $H \cap K$ since it belongs to the subgroups H and K. If x and y are elements of $H \cap K$ then xy is an element of H (since x and y are elements of H), and xy is an element of K, and therefore xy is an element of $H \cap K$. Also the inverse x^{-1} of an element x of $H \cap K$ belongs to H and to K and thus belongs to $H \cap K$, as required. ∎

More generally, the intersection of any collection of subgroups of a given group is itself a subgroup of that group.

2.5 Cyclic Groups

Definition A group G is said to be *cyclic*, with generator x, if every element of G is of the form x^n for some integer n.

Example The group $\mathbb{Z}$ of integers under addition is a cyclic group, generated by 1.

Example Let n be a positive integer. The set $\mathbb{Z}_n$ of congruence classes of integers modulo n is a cyclic group of order n with respect to the operation of addition.

Example The group of all rotations of the plane about the origin through an integer multiple of $2\pi/n$ radians is a cyclic group of order n for all integers n. This group is generated by an anticlockwise rotation through an angle of $2\pi/n$ radians.

2.6 Cosets and Lagrange's Theorem

Definition Let H be a subgroup of a group G. A *left coset* of H in G is a subset of G that is of the form xH, where $x \in G$ and

$$xH = \{y \in G : y = xh \text{ for some } h \in H\}.$$

Similarly a *right coset* of H in G is a subset of G that is of the form Hx, where $x \in G$ and

$$Hx = \{y \in G : y = hx \text{ for some } h \in H\}.$$

Note that a subgroup H of a group G is itself a left coset of H in G.

Lemma 2.7 *Let H be a subgroup of a group G. Then the left cosets of H in G have the following properties:—*

(i) *$x \in xH$ for all $x \in G$;*

(ii) *if x and y are elements of G, and if $y = xa$ for some $a \in H$, then $xH = yH$;*

(iii) *if x and y are elements of G, and if $xH \cap yH$ is non-empty then $xH = yH$.*

Proof Let $x \in G$. Then $x = xe$, where e is the identity element of G. But $e \in H$. It follows that $x \in xH$. This proves (i).

Let x and y be elements of G, where $y = xa$ for some $a \in H$. Then $yh = x(ah)$ and $xh = y(a^{-1}h)$ for all $h \in H$. Moreover $ah \in H$ and $a^{-1}h \in H$ for all $h \in H$, since H is a subgroup of G. It follows that $yH \subset xH$ and $xH \subset yH$, and hence $xH = yH$. This proves (ii).

Finally suppose that $xH \cap yH$ is non-empty for some elements x and y of G. Let z be an element of $xH \cap yH$. Then $z = xa$ for some $a \in H$, and $z = yb$ for some $b \in H$. It follows from (ii) that $zH = xH$ and $zH = yH$. Therefore $xH = yH$. This proves (iii). ∎

Lemma 2.8 *Let H be a finite subgroup of a group G. Then each left coset of H in G has the same number of elements as H.*

Proof Let $H = \{h_1, h_2, \ldots, h_m\}$, where $h_1, h_2, \ldots, h_m$ are distinct, and let x be an element of G. Then the left coset xH consists of the elements xh_j for $j = 1, 2, \ldots, m$. Suppose that j and k are integers between 1 and m for which $xh_j = xh_k$. Then $h_j = x^{-1}(xh_j) = x^{-1}(xh_k) = h_k$, and thus $j = k$, since $h_1, h_2, \ldots, h_m$ are distinct. It follows that the elements $xh_1, xh_2, \ldots, xh_m$ are distinct. We conclude that the subgroup H and the left coset xH both have m elements, as required. ∎

Theorem 2.9 (Lagrange's Theorem) *Let G be a finite group, and let H be a subgroup of G. Then the order of H divides the order of G.*

Proof Each element of G belongs to at least one left coset of H in G, and no element can belong to two distinct left cosets of H in G (see Lemma 2.7). Therefore every element of G belongs to exactly one left coset of H. Moreover each left coset of H contains $|H|$ elements (Lemma 2.8). Therefore $|G| = n|H|$, where n is the number of left cosets of H in G. The result follows. ∎

Definition Let H be a subgroup of a group G. If the number of left cosets of H in G is finite then the number of such cosets is referred to as the *index* of H in G, denoted by $[G: H]$.

The proof of Lagrange's Theorem shows that the index $[G: H]$ of a subgroup H of a finite group G is given by $[G: H] = |G|/|H|$.

Corollary 2.10 *Let x be an element of a finite group G. Then the order of x divides the order of G.*

Proof Let H be the set of all elements of G that are of the form x^n for some integer n. Then H is a subgroup of G (see Lemma 2.5), and the order of H is the order of x. But the order of H divides G by Lagrange's Theorem (Theorem 2.9). The result follows. ∎

Corollary 2.11 *Any finite group of prime order is cyclic.*

Proof Let G be a group of prime order, and let x be some element of G that is not the identity element. Then the order of x is greater than one and divides the order of G. But then the order of x must be equal to the order of G, since the latter is a prime number. Thus G is a cyclic group generated by x, as required. ∎

2.7 Normal Subgroups and Quotient Groups

Let A and B be subsets of a group G. The *product* AB of the sets A and B is defined by

$$AB = \{xy : x \in A \text{ and } y \in B\}.$$

We denote $\{x\}A$ and $A\{x\}$ by xA and Ax, for all elements x of G and subsets A of G. The Associative Law for multiplication of elements of G ensures that $(AB)C = A(BC)$ for all subsets A, B and C of G. We can therefore use the notation ABC to denote the products $(AB)C$ and $A(BC)$;

and we can use analogous notation to denote the product of four or more subsets of G.

If A, B and C are subsets of a group G, and if $A \subset B$ then clearly $AC \subset BC$ and $CA \subset CB$.

Note that if H is a subgroup of the group G and if x is an element of G then xH is the left coset of H in G that contains the element x. Similarly Hx is the right coset of H in G that contains the element x.

If H is a subgroup of G then $HH = H$. Indeed $HH \subset H$, since the product of two elements of a subgroup H is itself an element of H. Also $H \subset HH$ since $h = eh$ for any element h of H, where e, the identity element of G, belongs to H.

Definition A subgroup N of a group G is said to be a *normal subgroup* of G if $xnx^{-1} \in N$ for all $n \in N$ and $x \in G$.

The notation '$N \triangleleft G$' signifies 'N is a normal subgroup of G'.

Definition A non-trivial group G is said to be *simple* if the only normal subgroups of G are the whole of G and the trivial subgroup $\{e\}$ whose only element is the identity element e of G.

Lemma 2.12 *Every subgroup of an Abelian group is a normal subgroup.*

Proof Let N be a subgroup of an Abelian group G. Then

$$xnx^{-1} = (xn)x^{-1} = (nx)x^{-1} = n(xx^{-1}) = ne = n$$

for all $n \in N$ and $x \in G$, where e is the identity element of G. The result follows. ∎

Example Let S_3 be the group of permutations of the set $\{1, 2, 3\}$, and let H be the subgroup of S_3 consisting of the identity permutation and the transposition $(1\,2)$. Then H is not normal in G, since $(2\,3)^{-1}(1\,2)(2\,3) = (2\,3)(1\,2)(2\,3) = (1\,3)$ and $(1\,3)$ does not belong to the subgroup H.

Proposition 2.13 *A subgroup N of a group G is a normal subgroup of G if and only if $xNx^{-1} = N$ for all elements x of G.*

Proof Suppose that N is a normal subgroup of G. Let x be an element of G. Then $xNx^{-1} \subset N$. (This follows directly from the definition of a normal subgroup.) On replacing x by x^{-1} we see also that $x^{-1}Nx \subset N$, and thus $N = x(x^{-1}Nx)x^{-1} \subset xNx^{-1}$. Thus each of the sets N and xNx^{-1} is contained in the other, and therefore $xNx^{-1} = N$.

Conversely if N is a subgroup of G with the property that $xNx^{-1} = N$ for all $x \in G$, then it follows immediately from the definition of a normal subgroup that N is a normal subgroup of G. ∎

Corollary 2.14 *A subgroup N of a group G is a normal subgroup of G if and only if $xN = Nx$ for all elements x of G.*

Proof Let N be a subgroup of G, and let x be an element of G. If $xNx^{-1} = N$ then $xN = (xNx^{-1})x = Nx$. Conversely if $xN = Nx$ then $xNx^{-1} = Nxx^{-1} = Ne = N$, where e is the identity element of G. Thus $xN = Nx$ if and only if $xNx^{-1} = N$. It follows from Proposition 2.13 that a subgroup N of G is normal if and only if $xN = Nx$ for all elements x of G, as required. ∎

Let N be a normal subgroup of G. Corollary 2.14 shows that a subset of G is a left coset of N in G if and only if it is a right coset of N in G. We may therefore refer to the left and right cosets of a normal subgroup N as *cosets* of N in G (since it is not in this case necessary to distinguish between left and right cosets).

Lemma 2.15 *Let N be a normal subgroup of a group G and let x and y be elements of G. Then $(xN)(yN) = (xy)N$.*

Proof If N is a normal subgroup of G then $Ny = yN$, and therefore $(xN)(yN) = x(Ny)N = x(yN)N = (xy)(NN)$. But $NN = N$, since N is a subgroup of G. Therefore $(xN)(yN) = (xy)N$, as required. ∎

Proposition 2.16 *Let G be a group, and let N be a normal subgroup of G. Then the set of all cosets of N in G is a group under the operation of multiplication. The identity element of this group is N itself, and the inverse of a coset xN is the coset $x^{-1}N$ for any element x of G.*

Proof Let x, y and z be any elements of G. Then the product of the cosets xN and yN is the coset $(xy)N$. The subgroup N is itself a coset of N in G, since $N = eN$. Moreover

$$(xN)N = (xN)(eN) = (xe)N = xN,$$

$$N(xN) = (eN)(xN) = (ex)N = xN,$$

$$(xN)(x^{-1}N) = (xx^{-1})N = N,$$

$$(x^{-1}N)(xN) = (x^{-1}x)N = N.$$

for all elements x of G. Thus the group axioms are satisfied. ∎

Definition Let N be a normal subgroup of a group G. The *quotient group* G/N is defined to be the group of cosets of N in G under the operation of multiplication.

Example Consider the dihedral group D_8 of order 8, which we represent as the group of symmetries of a square in the plane with corners at the points whose Cartesian co-ordinates are $(1,1)$, $(-1,1)$, $(-1,-1)$ and $(1,-1)$. Then

$$D_8 = \{\mathbf{I}, \mathbf{R}, \mathbf{R}^2, \mathbf{R}^3, \mathbf{T}_1, \mathbf{T}_2, \mathbf{T}_3, \mathbf{T}_4\},$$

where $\mathbf{I}$ denotes the identity transformation, $\mathbf{R}$ denotes an anticlockwise rotation about the origin through a right angle, and $\mathbf{T}_1$, $\mathbf{T}_2$, $\mathbf{T}_3$ and $\mathbf{T}_4$ denote the reflections in the lines $y = 0$, $x = y$, $x = 0$ and $x = -y$ respectively. Let $N = \{\mathbf{I}, \mathbf{R}^2\}$. Then N is a subgroup of D_8. The left cosets of N in D_8 are N, A, B and C, where

$$A = \{\mathbf{R}, \mathbf{R}^3\}, \qquad B = \{\mathbf{T}_1, \mathbf{T}_3\}, \qquad C = \{\mathbf{T}_2, \mathbf{T}_4\}.$$

Moreover N, A, B and C are also the right cosets of N in D_8, and thus N is a normal subgroup of D_8. On multiplying the cosets A, B and C with one another we find that $AB = BA = C$, $AC = CA = B$ and $BC = CB = A$. The quotient group D_8/N consists of the set $\{N, A, B, C\}$, with the group operation just described.

2.8 Homomorphisms

Definition A homomorphism $\theta: G \to K$ from a group G to a group K is a function with the property that $\theta(g_1 * g_2) = \theta(g_1) * \theta(g_2)$ for all $g_1, g_2 \in G$, where $*$ denotes the group operation on G and on K.

Example Let q be an integer. The function from the group $\mathbb{Z}$ of integers to itself that sends each integer n to qn is a homomorphism.

Example Let x be an element of a group G. The function that sends each integer n to the element x^n is a homomorphism from the group $\mathbb{Z}$ of integers to G, since $x^{m+n} = x^m x^n$ for all integers m and n (Theorem 2.4).

Lemma 2.17 *Let $\theta: G \to K$ be a homomorphism. Then $\theta(e_G) = e_K$, where e_G and e_K denote the identity elements of the groups G and K. Also $\theta(x^{-1}) = \theta(x)^{-1}$ for all elements x of G.*

Proof Let $z = \theta(e_G)$. Then $z^2 = \theta(e_G)\theta(e_G) = \theta(e_G e_G) = \theta(e_G) = z$. The result that $\theta(e_G) = e_K$ now follows from the fact that an element z of K satisfies $z^2 = z$ if and only if z is the identity element of K.

Let x be an element of G. The element $\theta(x^{-1})$ satisfies $\theta(x)\theta(x^{-1}) = \theta(xx^{-1}) = \theta(e_G) = e_K$, and similarly $\theta(x^{-1})\theta(x) = e_K$. The uniqueness of the inverse of $\theta(x)$ now ensures that $\theta(x^{-1}) = \theta(x)^{-1}$. ∎

An *isomorphism* $\theta: G \to K$ between groups G and K is a homomorphism that is also a bijection mapping G onto K. Two groups G and K are *isomorphic* if there exists an isomorphism mapping G onto K.

Example Let D_6 be the group of symmetries of an equilateral triangle in the plane with vertices A, B and C, and let S_3 be the group of permutations of the set $\{A, B, C\}$. The function which sends a symmetry of the triangle to the corresponding permutation of its vertices is an isomorphism between the dihedral group D_6 of order 6 and the symmetric group S_3.

Example Let $\mathbb{R}$ be the group of real numbers with the operation of addition, and let $\mathbb{R}^+$ be the group of strictly positive real numbers with the operation of multiplication. The function $\exp: \mathbb{R} \to \mathbb{R}^+$ that sends each real number x to the positive real number e^x is an isomorphism: it is both a homomorphism of groups and a bijection. The inverse of this isomorphism is the function $\log: \mathbb{R}^+ \to \mathbb{R}$ that sends each strictly positive real number to its natural logarithm.

Here is some further terminology regarding homomorphisms:

- A *monomorphism* is an injective homomorphism.
- An *epimorphism* is a surjective homomorphism.
- An *endomorphism* is a homomorphism mapping a group into itself.
- An *automorphism* is an isomorphism mapping a group onto itself.

Definition The *kernel* $\ker\theta$ of the homomorphism $\theta: G \to K$ is the set of all elements of G that are mapped by θ onto the identity element of K.

Example Let the group operation on the set $\{+1, -1\}$ be multiplication, and let $\theta: \mathbb{Z} \to \{+1, -1\}$ be the homomorphism that sends each integer n to $(-1)^n$. Then the kernel of the homomorphism θ is the subgroup of $\mathbb{Z}$ consisting of all even numbers.

Lemma 2.18 *Let G and K be groups, and let $\theta: G \to K$ be a homomorphism from G to K. Then the kernel $\ker\theta$ of θ is a normal subgroup of G.*

Proof Let x and y be elements of $\ker\theta$. Then $\theta(x) = e_K$ and $\theta(y) = e_K$, where e_K denotes the identity element of K. But then $\theta(xy) = \theta(x)\theta(y) = e_K e_K = e_K$, and thus xy belongs to $\ker\theta$. Also $\theta(x^{-1}) = \theta(x)^{-1} = e_K^{-1} = e_K$, and thus x^{-1} belongs to $\ker\theta$. We conclude that $\ker\theta$ is a subgroup of K. Moreover $\ker\theta$ is a normal subgroup of G, for if $g \in G$ and $x \in \ker\theta$ then

$$\theta(gxg^{-1}) = \theta(g)\theta(x)\theta(g)^{-1} = \theta(g)\theta(g^{-1}) = e_K. \quad \blacksquare$$

If N is a normal subgroup of some group G then N is the kernel of the *quotient homomorphism* $\theta: G \to G/N$ that sends $g \in G$ to the coset gN. It follows therefore that a subset of a group G is a normal subgroup of G if and only if it is the kernel of some homomorphism.

Proposition 2.19 *Let G and K be groups, let $\theta: G \to K$ be a homomorphism from G to K, and let N be a normal subgroup of G. Suppose that $N \subset \ker \theta$. Then the homomorphism $\theta: G \to K$ induces a homomorphism $\hat{\theta}: G/N \to K$ sending $gN \in G/N$ to $\theta(g)$. Moreover $\hat{\theta}: G/N \to K$ is injective if and only if $N = \ker \theta$.*

Proof Let x and y be elements of G. Now $xN = yN$ if and only if $x^{-1}y \in N$. Also $\theta(x) = \theta(y)$ if and only if $x^{-1}y \in \ker \theta$. Thus if $N \subset \ker \theta$ then $\theta(x) = \theta(y)$ whenever $xN = yN$, and thus $\theta: G \to K$ induces a well-defined function $\hat{\theta}: G/N \to K$ sending $xN \in G/N$ to $\theta(x)$. This function is a homomorphism, since $\hat{\theta}((xN)(yN)) = \hat{\theta}(xyN) = \theta(xy) = \theta(x)\theta(y) = \hat{\theta}(xN)\hat{\theta}(yN)$.

Suppose now that $N = \ker \theta$. Then $\theta(x) = \theta(y)$ if and only if $xN = yN$. Thus the homomorphism $\hat{\theta}: G/N \to K$ is injective. Conversely if $\hat{\theta}: G/N \to K$ is injective then N must be the kernel of θ, as required. ∎

Corollary 2.20 *Let G and K be groups, and let $\theta: G \to K$ be a homomorphism. Then $\theta(G) \cong G/\ker \theta$.*

2.9 The Isomorphism Theorems

Lemma 2.21 *Let G be a group, let H be a subgroup of G, and let N be a normal subgroup of G. Then the set HN is a subgroup of G, where $HN = \{hn : h \in H \text{ and } n \in N\}$.*

Proof The set HN clearly contains the identity element of G. Let x and y be elements of HN. We must show that xy and x^{-1} belong to HN. Now $x = hu$ and $y = kv$ for some elements h and k of H and for some elements u and v of N. Then $xy = (hk)(k^{-1}ukv)$. But $k^{-1}uk \in N$, since N is normal. It follows that $k^{-1}ukv \in N$, since N is a subgroup and $k^{-1}ukv$ is the product of the elements $k^{-1}uk$ and v of N. Also $hk \in H$. It follows that $xy \in HN$.

We must also show that $x^{-1} \in HN$. Now $x^{-1} = u^{-1}h^{-1} = h^{-1}(hu^{-1}h^{-1})$. Also $h^{-1} \in H$, since H is a subgroup of G, and $hu^{-1}h^{-1} \in N$, since N is a normal subgroup of G. It follows that $x^{-1} \in HN$, and thus HN is a subgroup of G, as required. ∎

Theorem 2.22 (First Isomorphism Theorem) *Let G be a group, let H be a subgroup of G, and let N be a normal subgroup of G. Then*

$$\frac{HN}{N} \cong \frac{H}{N \cap H}.$$

Proof Every element of HN/N is a coset of N that is of the form hN for some $h \in H$. Thus if $\varphi(h) = hN$ for all $h \in H$ then $\varphi: H \to HN/N$ is a surjective homomorphism, and $\ker \varphi = N \cap H$. But $\varphi(H) \cong H/\ker \varphi$ (Corollary 2.20). Therefore $HN/N \cong H/(N \cap H)$ as required. ∎

Theorem 2.23 (Second Isomorphism Theorem) *Let M and N be normal subgroups of a group G, where $M \subset N$. Then*

$$\frac{G}{N} \cong \frac{G/M}{N/M}.$$

Proof There is a well-defined homomorphism $\theta: G/M \to G/N$ that sends gM to gN for all $g \in G$. Moreover the homomorphism θ is surjective, and $\ker \theta = N/M$. But $\theta(G/M) \cong (G/M)/\ker \theta$. Therefore G/N is isomorphic to $(G/M)\,/\,(N/M)$, as required. ∎

2.10 Group Actions, Orbits and Stabilizers

Definition A *left action* of a group G on a set X associates to each $g \in G$ and $x \in X$ an element $g.x$ of X in such a way that $g.(h.x) = (gh).x$ and $1.x = x$ for all $g, h \in G$ and $x \in X$, where 1 denotes the identity element of G.

Given a left action of a group G on a set X, the *orbit* of an element x of X is the subset $\{g.x : g \in G\}$ of X, and the *stabilizer* of x is the subgroup $\{g \in G : g.x = x\}$ of G.

Lemma 2.24 *Let G be a finite group which acts on a set X on the left. Then the orbit of an element x of X contains $[G: H]$ elements, where $[G: H]$ is the index of the stabilizer H of x in G.*

Proof There is a well-defined function $\theta: G/H \to X$ defined on the set G/H of left cosets of H in G which sends gH to $g.x$ for all $g \in G$. Moreover this function is injective, and its image is the orbit of x. The result follows. ∎

2.11 Conjugacy

Definition Two elements h and k of a group G are said to be *conjugate* if $k = ghg^{-1}$ for some $g \in G$.

One can readily verify that the relation of conjugacy is reflexive, symmetric and transitive and is thus an equivalence relation on a group G. The equivalence classes determined by this relation are referred to as the *conjugacy classes* of G. A group G is the disjoint union of its conjugacy classes. Moreover the conjugacy class of the identity element of G contains no other element of G.

A group G is Abelian if and only if all its conjugacy classes contain exactly one element of the group G.

Definition Let G be a group. The *centralizer* $C(h)$ of an element h of G is the subgroup of G defined by $C(h) = \{g \in G : gh = hg\}$.

Lemma 2.25 *Let G be a finite group, and let $h \in G$. Then the number of elements in the conjugacy class of h is equal to the index $[G\colon C(h)]$ of the centralizer $C(h)$ of h in G.*

Proof There is a well-defined function $f\colon G/C(h) \to G$, defined on the set $G/C(h)$ of left cosets of $C(h)$ in G, which sends the coset $gC(h)$ to ghg^{-1} for all $g \in G$. This function is injective, and its image is the conjugacy class of h. The result follows. ∎

Let H be a subgroup of a group G. One can easily verify that gHg^{-1} is also a subgroup of G for all $g \in G$, where $gHg^{-1} = \{ghg^{-1} : h \in H\}$.

Definition Two subgroups H and K of a group G are said to be *conjugate* if $K = gHg^{-1}$ for some $g \in G$.

The relation of conjugacy is an equivalence relation on the collection of subgroups of a given group G.

2.12 Finitely Generated Abelian Groups

Let H be a subgroup of the additive group $\mathbb{Z}^n$ consisting of all n-tuples of integers, with the operation of (vector) addition. A list $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_r$ of elements of $\mathbb{Z}^n$ is said to constitute an *integral basis* (or $\mathbb{Z}$*-basis*) of H if the following conditions are satisfied:

- the element $m_1\mathbf{b}_1 + m_2\mathbf{b}_2 + \cdots + m_r\mathbf{b}_r$ belongs to H for all integers $m_1, m_2, \ldots, m_r$;
- given any element $\mathbf{h}$ of H, there exist uniquely determined integers $m_1, m_2, \ldots, m_r$ such that $\mathbf{h} = m_1\mathbf{b}_1 + m_2\mathbf{b}_2 + \cdots + m_r\mathbf{b}_r$.

Note that elements $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ of $\mathbb{Z}^n$ constitute an integral basis of $\mathbb{Z}^n$ if and only if every element of $\mathbb{Z}^n$ is uniquely expressible as a linear combination of $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ with integer coefficients. It follows from basic linear algebra that the rows of an $n \times n$ matrix of integers constitute an integral basis of $\mathbb{Z}^n$ if and only if the determinant of that matrix is ± 1.

Theorem 2.26 *Let H be a non-trivial subgroup of $\mathbb{Z}^n$. Then there exists an integral basis $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ of $\mathbb{Z}^n$, a positive integer s, where $s \leq n$, and positive integers $k_1, k_2, \ldots, k_s$ for which $k_1\mathbf{b}_1, k_2\mathbf{b}_2, \ldots, k_s\mathbf{b}_s$ is an integral basis of H.*

Proof We prove the result by induction on n. The result is clearly true when $n = 1$, since every non-trivial subgroup of $\mathbb{Z}$ is of the form $k\mathbb{Z}$ for some positive integer k. Suppose therefore that $n > 1$ and that the result holds for all subgroups of $\mathbb{Z}^{n-1}$. We must show that the result then holds for all subgroups H of $\mathbb{Z}^n$.

Let k_1 be the smallest strictly positive integer for which there exists some integral basis $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n$ of $\mathbb{Z}^n$ and some element of H of the form $m_1\mathbf{u}_1 + m_2\mathbf{u}_2 + \cdots + m_n\mathbf{u}_n$ where $m_1, m_2, \ldots, m_n$ are integers and $m_i = k_1$ for some integer i satisfying $1 \leq i \leq n$. Let $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n$ be such a basis, with $i = 1$, and let $\mathbf{h}_0$ be an element of H for which $\mathbf{h}_0 = m_1\mathbf{u}_1 + m_2\mathbf{u}_2 + \cdots + m_n\mathbf{u}_n$, where $m_1, m_2, \ldots, m_n$ are integers and $m_1 = k_1$.

We show that each coefficient m_i is divisible by k_1. Now, for each i, there exist integers q_i and r_i such that $m_i = q_ik_1 + r_i$ and $0 \leq r_i < k_1$. Let $\mathbf{b}_1 = \mathbf{u}_1 + \sum_{i=2}^{n} q_i\mathbf{u}_i$. Then $\mathbf{b}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n$ is an integral basis of $\mathbb{Z}^n$ and

$$\mathbf{h}_0 = k_1\mathbf{b}_1 + \sum_{i=2}^{n} r_i\mathbf{u}_i.$$

The choice of k_1 now ensures that the coefficients r_i cannot be strictly positive (as they are less than k_1), and therefore $r_i = 0$ and $m_i = q_ik_1$ for $i = 2, 3, \ldots, n$. Moreover $\mathbf{h}_0 = k_1\mathbf{b}_1$.

Now let $\varphi\colon \mathbb{Z}^{n-1} \to \mathbb{Z}^n$ be the injective homomorphism sending each element $(m_2, m_3, \ldots, m_n)$ of $\mathbb{Z}^{n-1}$ to $\sum_{i=2}^{n} m_i\mathbf{u}_i$, and let $\tilde{H} = \varphi^{-1}(H)$. Then, given any element $\mathbf{h}$ of H, there exist an integer m and an element $\tilde{\mathbf{h}}$ of $\mathbb{Z}^{n-1}$ such that $\mathbf{h} = m\mathbf{b}_1 + \varphi(\tilde{\mathbf{h}})$. Moreover m and $\tilde{\mathbf{h}}$ are uniquely determined by

$\mathbf{h}$, since $\mathbf{b}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n$ is an integral basis of $\mathbb{Z}^n$. Let $m = qk_1 + r$, where q and r are integers and $0 \leq r < k_1$. Then $\mathbf{h} - q\mathbf{h}_0 = r\mathbf{b}_1 + \varphi(\tilde{\mathbf{h}})$, where $\varphi(\tilde{\mathbf{h}})$ is expressible as a linear combination of $\mathbf{u}_2, \ldots, \mathbf{u}_n$ with integer coefficients. The choice of k_1 now ensures that r cannot be strictly positive, and therefore $r = 0$. Then $\varphi(\tilde{\mathbf{h}}) \in H$, and hence $\tilde{\mathbf{h}} \in \tilde{H}$. We conclude from this that, given any element $\mathbf{h}$ of H, there exist an integer q and an element $\tilde{\mathbf{h}}$ of $\tilde{H}$ such that $\mathbf{h} = qk_1\mathbf{b}_1 + \varphi(\tilde{\mathbf{h}})$. Moreover q and $\tilde{\mathbf{h}}$ are uniquely determined by $\mathbf{h}$.

Now the induction hypothesis ensures the existence of an integral basis $\tilde{\mathbf{b}}_2, \tilde{\mathbf{b}}_3, \ldots, \tilde{\mathbf{b}}_n$ of $\mathbb{Z}^{n-1}$ for which there exist positive integers $k_2, k_3, \ldots, k_s$ such that $k_2\tilde{\mathbf{b}}_2, k_3\tilde{\mathbf{b}}_3, \ldots, k_s\tilde{\mathbf{b}}_s$ is an integral basis of $\tilde{H}$. Let $\mathbf{b}_i = \varphi(\tilde{\mathbf{b}}_i)$ for each integer i between 2 and n. One can then readily verify that $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ is an integral basis of $\mathbb{Z}^n$ and $k_1\mathbf{b}_1, k_2\mathbf{b}_2, \ldots, k_s\mathbf{b}_s$ is an integral basis of H, as required. ∎

An Abelian group G is generated by elements $g_1, g_2, \ldots, g_n$ if and only if every element of G is expressible in the form $g_1^{m_1} g_2^{m_2} \cdots g_n^{m_n}$ for some integers $m_1, m_2, \ldots, m_n$.

Lemma 2.27 *A non-trivial Abelian group G is finitely generated if and only if there exists a positive integer n and some surjective homomorphism $\theta\colon \mathbb{Z}^n \to G$.*

Proof Let $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n$ be the integral basis of $\mathbb{Z}^n$ with $\mathbf{e}_1 = (1, 0, \ldots, 0)$, $\mathbf{e}_2 = (0, 1, 0, \ldots, 0), \ldots,$ $\mathbf{e}_n = (0, \ldots, 0, 1)$. If there exists a surjective homomorphism $\theta\colon \mathbb{Z}^n \to G$ then G is generated by $g_1, g_2, \ldots, g_n$, where $g_i = \theta(\mathbf{e}_i)$ for $i = 1, 2, \ldots, n$. Conversely if G is generated by $g_1, g_2, \ldots, g_n$ then there is a surjective homomorphism $\theta\colon \mathbb{Z}^n \to G$ that sends $(m_1, m_2, \ldots, m_n) \in \mathbb{Z}^n$ to $g_1^{m_1} g_2^{m_2} \cdots g_n^{m_n}$. ∎

Theorem 2.28 *Let G be a non-trivial finitely generated Abelian group. Then there exist a positive integer n and a non-negative integer s between 0 and n, such that if $s = 0$ then $G \cong \mathbb{Z}^n$, and if $s > 0$ then there exist positive integers $k_1, k_2, \ldots, k_s$ such that*

$$G \cong C_{k_1} \times C_{k_2} \times \cdots \times C_{k_s} \times \mathbb{Z}^{n-s},$$

where C_{k_i} is a cyclic group of order k_i for $i = 1, 2, \ldots, s$.

Proof There exists a positive integer n and some surjective homomorphism $\theta\colon \mathbb{Z}^n \to G$, since G is finitely-generated. Let H be the kernel of θ. If H is trivial then the homomorphism θ is an isomorphism between $\mathbb{Z}^n$ and G. If H is non-trivial then G is isomorphic to $\mathbb{Z}^n/H$, and there exists an

integral basis $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ of $\mathbb{Z}^n$, a positive integer s, where $s \leq n$, and positive integers $k_1, k_2, \ldots, k_s$ for which $k_1\mathbf{b}_1, k_2\mathbf{b}_2, \ldots, k_s\mathbf{b}_s$ is an integral basis of H (Theorem 2.26). Then the group $\mathbb{Z}^n/H$, and thus G, is isomorphic to $C_{k_1} \times C_{k_2} \times \cdots \times C_{k_s} \times \mathbb{Z}^{n-s}$, where C_{k_i} is a cyclic group of order k_i for $i = 1, 2, \ldots, s$. Indeed there is a well-defined homomorphism $\varphi\colon \mathbb{Z}^n \to C_{k_1} \times C_{k_2} \times \cdots \times C_{k_s} \times \mathbb{Z}^{n-s}$ which sends each element

$$m_1\mathbf{b}_1 + m_2\mathbf{b}_2 + \cdots + m_n\mathbf{b}_n$$

of $\mathbb{Z}^n$ to $(a_1^{m_1}, a_2^{m_2}, \ldots, a_s^{m_s}, m_{s+1}, \ldots, m_n)$, where a_i is a generator of the cyclic group C_i for $i = 1, 2, \ldots, s$. The homomorphism φ is surjective, and its kernel is the subgroup H. Therefore $G \cong \mathbb{Z}^n/H \cong C_{k_1} \times C_{k_2} \times \cdots \times C_{k_s} \times \mathbb{Z}^{n-s}$, as required. ∎

Corollary 2.29 *Let G be a non-trivial finite Abelian group. Then there exist positive integers $k_1, k_2, \ldots, k_n$ such that $G \cong C_{k_1} \times C_{k_2} \times \cdots \times C_{k_n}$, where C_{k_i} is a cyclic group of order k_i for $i = 1, 2, \ldots, n$.*

With some more work it is possible to show that the positive integers $k_1, k_2, \ldots, k_s$ in Theorem 2.28 may be chosen such that $k_1 > 1$ and k_{i-1} divides k_i for $i = 2, 3, \ldots, s$, and that the Abelian group is then determined up to isomorphism by the integer n and the sequence of positive integers $k_1, k_2, \ldots, k_s$.

2.13 The Class Equation of a Finite Group

Definition The *centre* $Z(G)$ of a group G is the subgroup of G defined by

$$Z(G) = \{g \in G : gh = hg \text{ for all } h \in G\}.$$

One can verify that the centre of a group G is a normal subgroup of G.

Let G be a finite group, and let $Z(G)$ be the centre of G. Then $G \setminus Z(G)$ is a disjoint union of conjugacy classes. Let r be the number of conjugacy classes contained in $G \setminus Z(G)$, and let $n_1, n_2, \ldots, n_r$ be the number of elements in these conjugacy classes. Then $n_i > 1$ for all i, since the centre $Z(G)$ of G is the subgroup of G consisting of those elements of G whose conjugacy class contains just one element. Now the group G is the disjoint union of its conjugacy classes, and therefore

$$|G| = |Z(G)| + n_1 + n_2 + \cdots + n_r.$$

This equation is referred to as the *class equation* of the group G.

Definition Let g be an element of a group G. The *centralizer* $C(g)$ of g is the subgroup of G defined by $C(g) = \{h \in G : hg = gh\}$.

Proposition 2.30 *Let G be a finite group, and let p be a prime number. Suppose that p^k divides the order of G for some positive integer k. Then either p^k divides the order of some proper subgroup of G, or else p divides the order of the centre of G.*

Proof Choose elements $g_1, g_2, \ldots, g_r$ of $G \setminus Z(G)$, where $Z(G)$ is the centre of G, such that each conjugacy class included in $G \setminus Z(G)$ contains exactly one of these elements. Let n_i be the number of elements in the conjugacy class of g_i and let $C(g_i)$ be the centralizer of g_i for each i. Then $C(g_i)$ is a proper subgroup of G, and $|G| = n_i|C(g_i)|$. Thus if p^k divides $|G|$ but does not divide the order of any proper subgroup of G then p must divide n_i for $i = 1, 2, \ldots, r$. Examination of the class equation $|G| = |Z(G)| + n_1 + n_2 + \cdots + n_r$ now shows that p divides $|Z(G)|$, as required. ∎

2.14 Cauchy's Theorem

Theorem 2.31 (Cauchy) *Let G be an finite group, and let p be a prime number that divides the order of G. Then G contains an element of order p.*

Proof We prove the result by induction on the order of G. Thus suppose that every finite group whose order is divisible by p and less than $|G|$ contains an element of order p. If p divides the order of some proper subgroup of G then that subgroup contains the required element of order p. If p does not divide the order of any proper subgroup of G then Proposition 2.30 ensures that p divides the order of the centre $Z(G)$ of G, and thus $Z(G)$ cannot be a proper subgroup of G. But then $G = Z(G)$ and the group G is Abelian.

Thus let G be an Abelian group whose order is divisible by p, and let H be a proper subgroup of G that is not contained in any larger proper subgroup. If $|H|$ is divisible by p then the induction hypothesis ensures that H contains the required element of order p, since $|H| < |G|$. Suppose then that $|H|$ is not divisible by p. Choose $g \in G \setminus H$, and let C be the cyclic subgroup of G generated by g. Then $HC = G$, since $HC \neq H$ and HC is a subgroup of G containing H. It follows from the First Isomorphism Theorem (Theorem 2.22) that $G/H \cong C/H \cap C$. Now p divides $|G/H|$, since $|G/H| = |G|/|H|$ and p divides $|G|$ but not $|H|$. Therefore p divides $|C|$. Thus if $m = |C|/p$ then g^m is the required element of order p. This completes the proof of Cauchy's Theorem. ∎

2.15 The Structure of p-Groups

Definition Let p be a prime number. A *p-group* is a finite group whose order is some power p^k of p.

Lemma 2.32 *Let p be a prime number, and let G be a p-group. Then there exists a normal subgroup of G of order p that is contained in the centre of G.*

Proof Let $|G| = p^k$. Then p^k divides the order of G but does not divide the order of any proper subgroup of G. It follows from Proposition 2.30 that p divides the order of the centre of G. It then follows from Cauchy's Theorem (Theorem 2.31) that the centre of G contains some element of order p. This element generates a cyclic subgroup of order p, and this subgroup is normal since its elements commute with every element of G. ∎

Proposition 2.33 *Let G be a p-group, where p is some prime number, and let H be a proper subgroup of G. Then there exists some subgroup K of G such that $H \triangleleft K$ and K/H is a cyclic group of order p.*

Proof We prove the result by induction on the order of G. Thus suppose that the result holds for all p-groups whose order is less than that of G. Let Z be the centre of G. Then ZH is a well-defined subgroup of G, since Z is a normal subgroup of G.

Suppose that $ZH \neq H$. Then H is a normal subgroup of ZH. The quotient group ZH/H is a p-group, and contains a subgroup K_1 of order p (Lemma 2.32). Let $K = \{g \in ZH : gH \in K_1\}$. Then $H \triangleleft K$ and $K/H \cong K_1$, and therefore K is the required subgroup of G.

Finally suppose that $ZH = H$. Then $Z \subset H$. Let $H_1 = \{hZ : h \in H\}$. Then H_1 is a subgroup of G/Z. But G/Z is a p-group, and $|G/Z| < |G|$, since $|Z| \geq p$ (Lemma 2.32). The induction hypothesis ensures the existence of a subgroup K_1 of G/Z such that $H_1 \triangleleft K_1$ and K_1/H_1 is cyclic of order p. Let $K = \{g \in G : gZ \in K_1\}$. Then $H \triangleleft K$ and $K/H \cong K_1/H_1$. Thus K is the required subgroup of G. ∎

Repeated applications of Proposition 2.33 yield the following result.

Corollary 2.34 *Let G be a finite group whose order is a power of some prime number p. Then there exist subgroups $G_0, G_1, \ldots, G_n$ of G, where G_0 is the trivial subgroup and $G_n = G$, such that $G_{i-1} \triangleleft G_i$ and G_i/G_{i-1} is a cyclic group of order p for $i = 1, 2, \ldots, n$.*

2.16 The Sylow Theorems

Definition Let G be a finite group, and let p be a prime number dividing the order $|G|$ of G. A *p-subgroup* of G is a subgroup whose order is some power of p. A *Sylow p-subgroup* of G is a subgroup whose order is p^k, where k is the largest natural number for which p^k divides $|G|$.

Theorem 2.35 (First Sylow Theorem) *Let G be a finite group, and let p be a prime number dividing the order of G. Then G contains a Sylow p-subgroup.*

Proof We prove the result by induction on the order of G. Thus suppose that all groups whose order is less than that of G contain the required Sylow p-subgroups. Let k be the largest positive integer for which p^k divides $|G|$. If p^k divides the order of some proper subgroup H of G then the induction hypothesis ensures that H contains the required Sylow p-subgroup of order p^k. If p^k does not divide the order of any proper subgroup of G then p divides the order of the centre $Z(G)$ of G (Proposition 2.30). It follows from Cauchy's Theorem (Theorem 2.31) that $Z(G)$ contains an element of order p, and this element generates a normal subgroup N of G of order p. The induction hypothesis then ensures that G/N has a Sylow p-subgroup L of order p^{k-1}, since $|G/N| = |G|/p$. Let $K = \{g \in G : gN \in L\}$. Then $|K| = p|L| = p^k$, and thus K is the required Sylow p-subgroup of G. ∎

Theorem 2.36 (Second Sylow Theorem) *Let G be a finite group, and let p be a prime number dividing the order of G. Then all Sylow p-subgroups of G are conjugate, and any p-subgroup of G is contained in some Sylow p-subgroup of G. Moreover the number of Sylow p-subgroups in G divides the order of G and is congruent to 1 modulo p.*

Proof Let K be a Sylow p-subgroup of G, and let X be the set of left cosets of K in G. Let H be a p-subgroup of G. Then H acts on X on the left, where $h(gK) = hgK$ for all $h \in H$ and $g \in G$. Moreover $h(gK) = gK$ if and only if $g^{-1}hg \in K$. Thus an element gK of X is fixed by H if and only if $g^{-1}Hg \subset K$.

Let $|G| = p^k m$, where k and m are positive integers and m is coprime to p. Then $|K| = p^k$. Now the number of left cosets of K in G is $|G|/|K|$. Thus the set X has m elements. Now the number of elements in any orbit for the action of H on X divides the order of H, since it is the index in H of the stabilizer of some element of that orbit (Lemma 2.24). But then the number of elements in each orbit must be some power of p, since H is a p-group. Thus if an element of X is not fixed by H then the number of elements in its orbit is divisible by p. But X is a disjoint union of orbits under the action

of H on X. Thus if m' denotes the number of elements of X that are fixed by H then $m - m'$ is divisible by p.

Now m is not divisible by p. It follows that $m' \neq 0$, and m' is not divisible by p. Thus there exists at least one element g of G such that $g^{-1}Hg \subset K$. But then H is contained in the Sylow p-subgroup gKg^{-1}. Thus every p-subgroup is contained in a Sylow p-subgroup of G, and this Sylow p-subgroup is a conjugate of the given Sylow p-subgroup K. In particular any two Sylow p-subgroups are conjugate.

It only remains to show that the number of Sylow p-subgroups in G divides the order of $|G|$ and is congruent to 1 modulo p. On applying the above results with $H = K$, we see that $g^{-1}Kg = K$ for some $g \in G$ if and only if gK is a fixed point for the action of K on X. But the number of elements g of G for which gK is a fixed point is $m'|K|$, where m' is the number of fixed points in X. It follows that the number of elements g of G for which $g^{-1}Kg = K$ is $p^k m'$. But every Sylow p-subgroup of G is of the form $g^{-1}Kg$ for some $g \in G$. It follows that the number n of Sylow p-subgroups in G is given by $n = |G|/p^k m' = m/m'$. In particular n divides $|G|$. Now we have already shown that $m - m'$ is divisible by p. It follows that m' is coprime to p, since m is coprime to p. Also $m - m'$ is divisible by m', since $(m - m')/m' = n - 1$. Putting these results together, we see that $m - m'$ is divisible by $m'p$, and therefore $n - 1$ is divisible by p. Thus n divides $|G|$ and is congruent to 1 modulo p, as required. ∎

2.17 Some Applications of the Sylow Theorems

Theorem 2.37 *Let p and q be prime numbers, where $p < q$ and $q \not\equiv 1 \pmod{p}$. Then any group of order pq is cyclic.*

Proof Let G be a group of order pq. It follows from the First Sylow Theorem that G contains Sylow subgroups N_p and N_q of orders p and q respectively. Now the number n_p of Sylow p-subgroups divides pq and satisfies $n_p \equiv 1 \pmod{p}$, by the Second Sylow Theorem. Clearly n_p cannot be divisible by p, and therefore either $n_p = 1$ or $n_p = q$. But $q \not\equiv 1 \pmod{p}$. It follows that $n_p = 1$. Thus the group G has just one subgroup of order p.

Now, given any element g of G, the subgroups N_p and gN_pg^{-1} are of order p. It follows that $gN_pg^{-1} = N_p$ for all elements g of G. Thus N_p is a normal subgroup of G.

A similar argument shows that N_q is also a normal subgroup of G, since $p < q$, and therefore $p \not\equiv 1 \pmod{q}$.

Now $N_p \cap N_q$ is a subgroup of both N_p and N_q. It follows from Lagrange's Theorem that the order of $N_p \cap N_q$ divides both of the prime numbers p and

q, and therefore $|N_p \cap N_q| = 1$ and $N_p \cap N_q = \{e\}$, where e is the identity element of G.

Let $x \in N_p$ and $y \in N_q$. Then $yx^{-1}y^{-1} \in N_p$ and $xyx^{-1} \in N_q$, since N_p and N_q are normal subgroups of G. But then $xyx^{-1}y^{-1} \in N_p \cap N_q$, since $xyx^{-1}y^{-1} = x(yx^{-1}y^{-1}) = (xyx^{-1})y^{-1}$, and therefore $xyx^{-1}y^{-1} = e$. Thus $xy = yx$ for all $x \in N_p$ and $y \in N_q$. It follows easily from this that the function $\varphi\colon N_p \times N_q \to G$ which sends $(x, y) \in N_p \times N_q$ to xy is a homomorphism. This homomorphism is injective, for if $xy = e$ for some $x \in N_p$ and $y \in N_q$, then $x = y^{-1}$, and hence $x \in N_p \cap N_q$, from which it follows that $x = e$ and $y = e$. But any injective homomorphism between two finite groups of the same order is necessarily an isomorphism. Therefore the function $\varphi\colon N_p \times N_q \to G$ is an isomorphism, and thus $G \cong N_p \times N_q$.

Now any group whose order is prime number must be cyclic. Therefore the groups N_p and N_q are cyclic. Let x be an element of N_p that generates N_p, and let y be an element of N_q that generates N_q. Then $(x, y)^n = (x^n, y^n)$ for all integers n. It follows from this that the order of (x, y) cannot be equal to 1, p or q, and must therefore be equal to pq. Thus $N_p \times N_q$ is a cyclic group generated by (x, y), and therefore G is a cyclic group, generated by xy, as required. ∎

Example Any finite group whose order is 15, 33, 35, 51, 65, 69, 85, 87, 91 or 95 is cyclic.

Theorem 2.38 *Let G be a group of order $2p$ where p is a prime number greater than 2. Then either the group G is cyclic, or else the group G is isomorphic to the dihedral group D_{2p} of symmetries of a regular p-sided polygon in the plane.*

Proof It follows from the First Sylow Theorem, or from Cauchy's Theorem, that the group G contains elements x and y whose orders are 2 and p respectively. The subgroup N generated by y is then a Sylow p-subgroup of G. Now it follows from the Second Sylow Theorem that the number of Sylow p-subgroups of G divides $2p$ and is congruent to 1 modulo p. There can therefore be only one such Sylow p-subgroup, since 2, p and $2p$ are not congruent to 1 modulo p. Now if g is any element of G then gNg^{-1} is a Sylow p-subgroup of G, and therefore $gNg^{-1} = N$. We deduce that N is a normal subgroup of G, of order p.

Now consider the element xyx^{-1} of G. This must be an element of the normal subgroup N of G generated by y. Therefore $xyx^{-1} = y^k$ for some integer k. Moreover k is not divisible by p, since xyx^{-1} is not the identity element e of G. Then

$$y^{k^2} = (y^k)^k = (xyx^{-1})^k = xy^kx^{-1} = x(xyx^{-1})x^{-1} = x^2yx^{-2}.$$

But $x^2 = x^{-2} = e$, since x is an element of G of order 2. It follows that $y^{k^2} = y$, and thus $y^{k^2-1} = e$. But then p divides $k^2 - 1$, since y is an element of order p. Moreover $k^2 - 1 = (k-1)(k+1)$. It follows that either p divides $k-1$, in which case $xyx^{-1} = y$, or else p divides $k+1$, in which case $xyx^{-1} = y^{-1}$.

In the case when $xyx^{-1} = y$ we see that $xy = yx$, and one can then readily verify that the group G is a cyclic group of order $2p$ generated by xy.

In the case when $xyx^{-1} = y^{-1}$ the group G is isomorphic to the dihedral group D_{2p} of order $2p$. In this case the elements x and y generate G (since they generate a subgroup of G whose order divides $2p$ but is greater than p, and must therefore be equal to $2p$). Under the isomorphism with the dihedral group D_{2p} the element x corresponds to a reflection in one of the axes of symmetry of the regular p-sided polygon, and the element y corresponds to a rotation of that polygon about its centre through an angle of $2\pi/p$ radians. ∎

Theorem 2.39 *Let p and q be prime numbers with $p < q$, and let d be the smallest positive integer for which $p^d \equiv 1 \pmod{q}$. If G is a group of order $p^k q$, where $0 < k < d$ then G contains a normal subgroup of order q. If G is a group of order $p^d q$ then either G contains a normal subgroup of order q or else G contains a normal subgroup of order p^d.*

Proof It follows from the First Sylow Theorem (or directly from Cauchy's Theorem) that the group G contains at least one Sylow q-subgroup K, and this is of order q. If $|G| = p^k q$ then the number n_q of such Sylow q-subgroups divides $p^k q$ and satisfies $n_q \equiv 1 \pmod{q}$, by the Second Sylow Theorem. It follows that n_q is coprime to q, and therefore $n_q = p^j$ for some integer j satisfying $0 \leq j \leq k$.

If $k < d$ then none of the integers $p, p^2, \ldots, p^k$ are congruent to 1 modulo q, and therefore $j = 0$ and $n_q = 1$. In this case there is just one Sylow q-subgroup K, and this is a normal subgroup. (Given any element g of G, the subgroup gKg^{-1} is a Sylow q-subgroup, and therefore $gKg^{-1} = K$.)

If $k = d$ then none of the integers p^j with $0 < j < d$ are congruent to 1 modulo q, and therefore either $n_q = 1$ or $n_q = p^d$. If $n_q = 1$ then there is just one Sylow q-subgroup K, and this is a normal subgroup.

If $n_q > 1$ then $n_q = p^d$, and thus there are p^d Sylow q-subgroups, and these are of order q. Now if K_i and K_j are two distinct subgroups of order q then $K_i \cap K_j$ is a proper subgroup of both K_i and K_j, and its order is a proper divisor of the order q of K_i and K_j, by Lagrange's Theorem. But q is a prime number. It follows that $K_i \cap K_j = \{e\}$, where e is the identity element of G. We deduce from this that no element of G of order q can belong to more than one subgroup of order q. But each subgroup of G of order q

contains $q-1$ elements of order q (namely all elements of that subgroup with the exception of the identity element). It follows that the group G contains $p^d(q-1)$ elements of order q. Now $|G| = p^d q$. It follows that G contains exactly p^d elements that are not of order q. But it follows from the First Sylow Theorem that G contains at least one Sylow p-subgroup H, and this is of order p^d. This subgroup must therefore contain all the elements of G that are not of order q. It follows that the group G cannot contain more than one such Sylow p-subgroup. This Sylow p-subgroup H is therefore a normal subgroup of G of order p^d, as required. ∎

2.18 Simple Groups

Definition A non-trivial group G is said to be *simple* if the only normal subgroups of G are the whole of G and the trivial subgroup $\{e\}$ whose only element is the identity element e of G.

Lemma 2.40 *Any non-trivial Abelian simple group is a cyclic group whose order is a prime number.*

Proof Let G be a non-trivial Abelian simple group, and let x be an element of G that is not equal to the identity element e of G. All subgroups of an Abelian group are normal subgroups. Therefore the subgroup of G generated by x is a normal subgroup of G, and must therefore be the whole of G. Therefore G is a cyclic group, generated by the element x. Moreover all elements of G other than the identity element are generators of G, and are therefore of order p, where $p = |G|$. Let d be a divisor of p. Then x^d is an element of order p/d, since p/d is the smallest positive integer k for which $x^{dk} = e$. It follows that either $d = 1$ or $d = p$ (since the group G contains no element whose order is greater than 1 but less than p). It follows that the order p of G is a prime number, as required. ∎

Using the Sylow Theorems and related results, we can prove that any finite simple group whose order is less than 60 is a cyclic group of prime order.

Now the prime numbers less than 60 are the following: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53 and 59. All groups of these orders are simple groups, and are cyclic groups.

If p is a prime number greater than 2 then any group of order $2p$ is either a cyclic group or else is isomorphic to the dihedral group D_{2p} of order $2p$ (Theorem 2.38). In either case such a group contains a normal subgroup of order p, and therefore not a simple group. In particular, there are no simple groups of orders 6, 10, 14, 22, 26, 34, 38, 46 or 58.

If G is a group of order p^k for some prime number p and for some integer k satisfying $k \geq 2$, then G contains a normal subgroup of order p (Lemma 2.32). It follows that such a group is not simple. In particular, there are no simple groups of orders 4, 8, 16, 32, 9, 27, 25 and 49.

Let G be a group of order pq, where p and q are prime numbers and $p < q$. Any Sylow q-subgroup of G is of order q, and the number of such Sylow q-subgroups must divide pq and be congruent to 1 modulo q. Now p cannot be congruent to 1 modulo q, since $1 < p < q$. Therefore G has just one Sylow q-subgroup, and this is a normal subgroup of G of order q. It follows that such a group is not a simple group. In particular there are no simple groups of orders 15, 21, 33, 35, 39, 51, 55 or 57. (In particular it follows from Theorem 2.37 that any group whose order is 15, 33, 35, or 51 is a cyclic group.)

It only remains to verify that there are no simple groups of orders 12, 18, 20, 24, 28, 30, 36, 40, 42, 44, 45, 48, 50, 52, 54 or 56.

We can deal with many of these on applying Theorem 2.39. On applying this theorem with $p = 2$, $q = 3$ and $d = 2$, we see that there are no simple groups of orders 6 or 12. On applying the theorem with $p = 2$, $q = 5$ and $d = 4$, we see that there are no simple groups of orders 10, 20, 40 or 80. On applying the theorem with $p = 2$, $q = 7$ and $d = 3$, we see that there are no simple groups of orders 14, 28 or 56. On applying the theorem with $p = 2$, $q = 11$ we see that there are no simple groups of orders 22, 44 etc., on applying the theorem with $p = 2$, $q = 13$ we see that there are no simple groups of orders 26, 52 etc., and on applying the theorem with $p = 3$ and $q = 5$, we see that there are no simple groups of orders 15, 45 etc.

It now remains to verify that there are no simple groups of orders 18, 24, 30, 36, 42, 48, 50 or 54.

Using the Second Sylow Theorem, we see that any group of order 18 has just one Sylow 3-subgroup. This Sylow 3-subgroup is then a normal group of order 9, and therefore no group of order 18 is simple. Similarly a group of order 50 has just one Sylow 5-subgroup, which is then a normal subgroup of order 25, and therefore no group of order 50 is simple. Also a group of order 54 has just one Sylow 3-subgroup, which is then a normal subgroup of order 27, and therefore no group of order 54 is simple.

On applying the Second Sylow Theorem, we see the number of Sylow 7-subgroups of any group of order 42 must divide 42 and be congruent to 1 modulo 7. This number must then be coprime to 7 and therefore divide 6, since $42 = 7 \times 6$. But no divisor of 6 greater than 1 is coprime to 1 modulo 7. It follows that any group of order 42 has just one Sylow 7-subgroup, and this subgroup is therefore a normal subgroup of order 7. Thus no group of order 42 is simple.

On applying the Second Sylow Theorem, we see that if a group of order 30 has more than one subgroup of order 3 then it must have 10 such subgroups, and must therefore have 20 elements of order 3 (since each subgroup of order 3 contains two elements of order 3, and the intersection of two distinct subgroups of order 3 must be the trivial subgroup). Similarly if a group of order 30 has more than one subgroup of order 5 then it must have 6 such subgroups, and must therefore have 24 elements of order 5. Obviously such a group cannot have both 20 elements of order 3 and 24 elements of order 5. Therefore it either has a single subgroup of order 3 or a single subgroup of order 5. This subgroup is normal. Therefore no group of order 30 is simple.

In order to show that there are no simple groups of order less than 60, apart from the cyclic groups whose order is prime, it only remains to verify that there are no simple groups of orders 24, 36 and 48. In order to deal with these remaining cases, we need to make use of the following result.

Lemma 2.41 *Let H and K be subgroups of a finite group G. Then*

$$|H \cap K| \geq \frac{|H|\,|K|}{|G|}.$$

Proof Let $\varphi: H \times K \to G$ be the function with $\varphi(h,k) = hk$ for all $h \in H$ and $k \in K$. (This function is not in general a homomorphism.) Let (h_1, k_1) and (h_2, k_2) be elements of $H \times K$. Then $h_1 k_1 = h_2 k_2$ if and only if $h_2^{-1} h_1 = k_2 k_1^{-1}$, in which case $h_2^{-1} h_1 \in H \cap K$. But then $h_2 = h_1 x^{-1}$ and $k_2 = x k_1$ for some element x of $H \cap K$. Thus $\varphi(h_1, k_1) = \varphi(h_2, k_2)$ if and only if $(h_2, k_2) = (h_1 x^{-1}, x k_1)$ for some element x of $H \cap K$. It follows that each element of the range $\varphi(H \times K)$ of the function φ is the image of exactly $|H \cap K|$ elements of $H \times K$. It follows from this that $\varphi(H \times K)$ has $\dfrac{|H|\,|K|}{|H \cap K|}$ elements. But $\varphi(H \times K)$ is a subset of G. Therefore

$$\frac{|H|\,|K|}{|H \cap K|} \leq |G|.$$

The required inequality now follows directly. ∎

Let G be a finite group, and let H be a subgroup of index 2 in G (i.e., a subgroup with half as many elements as G). Then H is a normal subgroup of G. Indeed the subsets H and $G \setminus H$ of G are the left cosets and are also the right cosets of H in G, and therefore the left cosets of H in G coincide with the right cosets.

Example We now show that there are no simple groups of order 24. Let G be a group of order 24. Then G contains a Sylow 2-subgroup H of order 8. If this is the only Sylow 2-subgroup, then it is a normal subgroup, and therefore the group G is not simple. Otherwise the group G contains at least two distinct subgroups H and K of order 8. It then follows from Lemma 2.41 that $|H \cap K| \geq \frac{8}{3}$. But $|H \cap K|$ divides 8, by Lagrange's Theorem, since $H \cap K$ is a subgroup of H and of K. Therefore $|H \cap K| = 4$. It follows that $H \cap K$ is a subgroup of index 2 in H and K, and is therefore a normal subgroup of both H and K. Let

$$J = \{g \in G : g(H \cap K)g^{-1} = H \cap K\}.$$

Then J is a subgroup of G, and $H \cap K$ is a normal subgroup of J. Moreover H and K are subgroups of J, and therefore $|J|$ is divisible by 8, by Lagrange's Theorem. But J is a subgroup of G, and hence $|J|$ divides 24. Also $|J| > 8$, since H (and K) are proper subgroups of J. It follows that $|J| = 24$, and therefore $J = G$. But then $H \cap K$ is a normal subgroup of G of order 4, and therefore G is not simple.

An analogous argument shows that there are no simple groups of order 48: a group G of order 48 contains either a single Sylow 2-subgroup of order 16, which is then a normal subgroup of G, or else it contains a normal subgroup of order 8 which is the intersection of two distinct Sylow 2-subgroups of G.

The following result will be needed in order to show that there are no simple groups of order 36. (It may be obtained as an immediate corollary of Proposition 2.33.)

Lemma 2.42 *Let G be a group of order p^2 where p is a prime number, and let H be a subgroup of G of order p. Then H is a normal subgroup of G.*

Proof Let $J = \{g \in G : gHg^{-1} = H\}$. Then J is a subgroup of G and H is a normal subgroup of J. We shall show that $J = G$.

Now the centre $Z(G)$ of G is contained in J. Moreover it follows from Lemma 2.32 that $|Z(G)|$ is divisible by p. Were it the case that $|J| = p$ then $J = H = Z(G)$. But then J would consist of all elements of G for which $gZ(G)g^{-1} = Z(G)$, and thus would be the whole of G, which is impossible. It follows that $|J| = p^2$ (since $|J| > p$ and $|J|$ divides p^2). But then $J = G$, and hence H is a normal subgroup of G, as required. ∎

Example We now show that there are no simple groups of order 36. Let G be a group of order 36. Then G contains a Sylow 3-subgroup H of order 9. If this is the only Sylow 3-subgroup, then it is a normal subgroup, and therefore

the group G is not simple. Otherwise the group G contains at least two distinct subgroups H and K of order 9. It then follows from Lemma 2.41 that $|H \cap K| \geq \frac{9}{4}$. But $|H \cap K|$ divides 9, by Lagrange's Theorem, since $H \cap K$ is a subgroup of H and of K. Therefore $|H \cap K| = 3$. On applying Lemma 2.42 we see that $H \cap K$ is a normal subgroup of H and of K.

Let

$$J = \{g \in G : g(H \cap K)g^{-1} = H \cap K\}.$$

Then J is a subgroup of G, and $H \cap K$ is a normal subgroup of J. Moreover H and K are subgroups of J, and therefore $|J|$ is divisible by 9, by Lagrange's Theorem. But J is a subgroup of G, and hence $|J|$ divides 36. Also $|J| > 9$, since H (and K) are proper groups of J. It follows that either $|J| = 18$ or 36. If $|J| = 36$ then $J = G$ and $H \cap K$ is a normal subgroup of G of order 3. If $|J| = 18$ then J is a subgroup of G of index 2, and is therefore a normal subgroup of order 18. We conclude that any group of order 36 contains at least one non-trivial normal subgroup. Therefore there are no simple groups of order 36.

We have now shown that there are indeed no simple groups of order less than 60, other than the cyclic groups of prime order.

There is a simple group of order 60 which is simple but is not cyclic. This group is the *alternating group* A_5, consisting of all even permutations of a set with five elements.

Lemma 2.43 *The alternating group A_5 is simple.*

Proof We regard A_5 as the group even permutations of the set $\{1, 2, 3, 4, 5\}$. There are 60 such permutations: the identity permutation, twenty 3-cycles, twenty-four 5-cycles, and fifteen permutations that are products of two disjoint transpositions. (Such a product of disjoint transpositions is a permutation $(a_1\, a_2)(a_3\, a_4)$ that interchanges a_1 with a_2 and a_3 with a_4 for some distinct elements a_1, a_2, a_3 and a_4 of the set $\{1, 2, 3, 4, 5\}$.)

Now each 3-cycle in A_5 generates a Sylow 3-subgroup of order 3, and these subgroups are all conjugate to one another by the Second Sylow Theorem. It follows that any normal subgroup of A_5 that contains at least one 3-cycle must contain all twenty 3-cycles, and thus its order must therefore be at least 21 (since it must also contain the identity element). Similarly each 5-cycle in A_5 generates a Sylow 5-subgroup of order 5, and these subgroups are all conjugate to one another. Therefore any normal subgroup of A_5 that contains at least one 5-cycle must contain all twenty four 5-cycles, and thus its order must be at least 25.

Now if A_5 were to contain a subgroup of order 30, this subgroup would be the kernel of a non-constant homomorphism $\varphi: A_5 \to \{1, -1\}$ from A_5 to the multiplicative group consisting of the numbers 1 and -1. But any 3-cycle or 5-cycle would have to belong to the kernel of this homomorphism, and therefore this kernel would contain at least 45 elements, which is impossible. We conclude that A_5 cannot contain any subgroup of order 30. It follows from Lagrange's Theorem that any normal subgroup of A_5 that contains at least one 3-cycle or 5-cycle must be the whole of A_5.

The group A_5 contains 5 Sylow 2-subgroups, which are of order 4. One of these consists of the identity permutation, together with the three permutations $(1\,2)(3\,4)$, $(1\,3)(2\,4)$ and $(1\,4)(2\,3)$. (Each of these permutations fixes the element 5.) There are four other such Sylow 2-subgroups, and all of the Sylow 2-subgroups are conjugate to one another. It follows that A_5 does not contain any normal subgroup of order 4. Moreover A_5 cannot contain any normal subgroup of order 2, since any element of order 2 belongs to one of the five Sylow 2-subgroups of order 4, and is therefore conjugate to elements of order 2 in the other Sylow 2-subgroups.

Now any subgroup of A_5 whose order is divisible by 3 must contain a 3-cycle by Cauchy's Theorem. (Theorem 2.31.) Similarly any subgroup of A_5 whose order is divisible by 5 must contain a 5-cycle. It follows that the order of any proper normal subgroup of A_5 cannot be divisible by 3 or 5. But this order must divide 60. Therefore the order of any proper normal subgroup of A_5 must be at most 4. But we have seen that A_5 cannot contain any normal subgroup of order 4 or 2. Therefore any proper normal subgroup of A_5 is trivial, and therefore A_5 is simple. ∎